UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/023,043	12/17/2001	David E. McDysan	RIC01059	5663

25537 7590 12/15/2004

MCI, INC
TECHNOLOGY LAW DEPARTMENT
1133 19TH STREET NW, 10TH FLOOR
WASHINGTON, DC 20036

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 12/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/023,043	MCDYSAN, DAVID E.	
	Examiner	Art Unit	
	Tom Gyorfi	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The communication filed on 6/25/04 did not add, cancel, or modify any claims. Claims 1-21 remain pending for examination.

Response to Arguments

2. Applicant's arguments filed 6/25/04 have been fully considered but they are not persuasive.

Applicant argues, "*...there is no disclosure [in the Tabata reference] that the ingress edge node is coupled to the egress edge node, as would be required by claim 1.*" Examiner disagrees with this contention, as Liu clearly teaches that it is possible for an edge node to perform both functions (paragraph 0046, lines 6-8); in this embodiment of the invention, it is apparent that the ingress edge node is coupled to the egress edge node. Further, it can be seen in Figure 1 of Tabata that all edge nodes are coupled to each other by the backbone network (element 3 of Figure 1).

3. Applicant argues, "*...there is no suggestion or disclosure [in the Liu reference] of 'separate access network logical connections for intra-VPN and extra-VPN traffic' as recited by claim 1.*" Examiner disagrees with this contention. Liu teaches that there is a clear distinction to be made between intra-VPN and extra-VPN traffic (col. 7, lines 30-40). It is also well known in the art and implicitly understood that IP-enabled devices are able to send traffic among multiple separate logical ports, which can be construed to be logical connections under the broadest definition of the term. Thus, at the bare minimum the

suggestion exists in Liu that separate access network logical connections for intra- and extra-VPN traffic would have been obvious to one of ordinary skill in the art to implement for Liu. Furthermore, Applicant is reminded that the rejection of claim 1 is based on the teachings of Liu as modified by the teachings of Tabata. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

4. Applicant argues, "*In contrast, claim 1 recites 'logically partitioning intra-VPN and extra-VPN traffic,' which is nowhere suggested or disclosed by Tabata. Moreover, Tabata's limiting of the input bandwidth of an in-network packet does not satisfy ' a plurality of ingress boundary routers coupled to the one ore more egress boundary routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic,* ***such that denial of service attacks on said access link originating from sources outside the VPN can be prevented'*** *as recited by claim 1, since the restriction on bandwidth occurs on* ***in-network packets*** *according to predetermined quality control information to perform control such that an in-network packet exceeding the bandwidth based on a contract with a user is not transmitted to the backbone network of Tabata. (par. 0026) This deficiency is not cured by any reasonable combination of Liu and Tabata.*" Examiner contends that this would have been an obvious development for one of ordinary skill in the art at the time the invention was made to implement. Note that the invention by Tabata routes packets according to quality control information received by the policy server as well as the Destination IP address found in the in-network packet header (paras. 0090 and 0096). It is well known in the art that all IP packets possess a "Destination IP address" field in the IPv4 header, including those designated "in-network" packets by Tabata (Figure 2).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the Destination IP address field found in the IPv4 header, as opposed to the one found in the in-network header (Figure 3) as the basis for determining whether the packet should be discarded in accordance with the quality control information, with the motivation being to prevent denial of service attacks on an access link from sources outside the VPN.

5. Applicant's arguments regarding the rejections of independent claims 9 and 16, as well as dependent claims 2-8, 10-15, and 17-20 have been fully considered but are not persuasive, based on the same grounds as cited in the preceding paragraph.

6. Applicant argues, "*In its rejection of claim 21, the Office Action asserts that it would have been obvious to 'modify the teachings of Liu such that precedence information is used to partition the traffic,' and that the motivation would be to 'prevent a bandwidth consumption attack.' (Office Action, page 7) However, the system of Liu examines packets to determine whether or not they are VPN traffic. Packets determined to be VPN traffic are processed for compression, encryption, and authentication rules according to the packet's VPN group, and packets determined to be non-VPN traffic are either passed through or discarded. (col 8: 17-39) The system of Tabata restricts the bandwidth for in-network packets according to predetermined quality control information to perform control such that an in-network packet exceeding the bandwidth based on a contract with the user is not transmitted to the backbone network of Tabata. (par. 0026) This is done to 'secure a required bandwidth for each end user' in order to ensure a communication bandwidth available to each end user for quality control. (pars. 0007 and 0010) Even if the two references were combinable, this type of modification to the system of Liu would do no more than ensure a communication bandwidth to each end user for quality control, and would not resist 'denial of service attacks on an access link to a destination host included in a VPN.' This deficiency is not satisfied by any reasonable combination of Liu and Tabata.*" Examiner disagrees with this contention, as

it would have been obvious to one of ordinary skill in the art at the time the invention was made to allow for the possibility. Again it should be noted that the primary determinant for a packet to be passed or dropped in accordance with the quality control information is the Destination IP Address (Tabata, paragraphs 0057, 0090, and 0096). This field is not endemic to the in-network packet header but was well known in the art as being a required field in all IPv4 packet headers, including the packets used in Tabata (Tabata, Figure 2). In addition, given that the backbone network depicted in Figure 1 of Tabata is identified as the Internet, it would be reasonable to assume that any node connected to the backbone network would be capable of instigating a denial of service attack against a particular node, regardless of whether the attacking node is a member of the same VPN as the defending node. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined teachings of Liu and Tabata to make a quality control determination of all packets sent to a node, and not simply those that are in-network, by using the Destination IP Address field in the IP header rather than the Destination IP Address found in the in-network header. The motivation for this would be to help defend against denial of service attacks instigated from outside the VPN.

Claim Rejections - 35 USC § 103

7. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

8. Claims 1-21 are rejected as being unpatentable over US 6079020 issued to Liu, herein referred to as Liu in view of US 2001/0016914 issued to Tabata, herein referred to as Tabata.

Referring to Claim 1:

Liu disclose a network system that resists denial of service attacks on an access link to a destination host belonging to a virtual private network (VPN), said network system comprising:

one or more egress boundary routers having connections to an access network including the access link (Fig. 1), wherein said one or more egress boundary routers transmit intra-VPN traffic from sources within the VPN and extra-VPN traffic from sources outside the VPN within separate access network logical connections for intra-VPN and extra-VPN traffic (col 7, lines 20-45; Fig 2); and

Liu does not explicitly disclose "a plurality of ingress boundary routers coupled to the one or more egress boundary routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, such that denial of service attacks on said access link originating from sources outside the VPN can be prevented".

Tabata discloses a plurality of ingress boundary routers coupled to the one or more egress boundary routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic (paragraph 0046, 0048;

paragraph 0084; paragraph 0091), such that denial of service attacks on said access link originating from sources outside the VPN can be prevented (paragraph 0084).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Liu such that a denial of service attack is prevented. One of ordinary skill in the art would have been motivated to do this because it would prevent a bandwidth consumption attack (Tabata: paragraph 0084).

Referring to Claim 9:

Liu discloses a network system, comprising: an access network having an access link to a destination host belonging to a virtual private network (VPN), wherein said access network supports a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN traffic from sources outside the VPN (col 7, lines 20-45; Fig. 1-2);

Liu does not explicitly disclose "one or more egress boundary routers having connections to the access network, wherein said one or more egress boundary routers transmit intra-VPN traffic toward the destination host via the first logical connection and transmit extra-VPN traffic toward the destination host via the second logical connection; a plurality of ingress boundary routers coupled to the one or more egress boundary routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, such that denial of service attacks on said access link originating from sources outside the VPN can be prevented"

Tabata discloses one or more egress boundary routers having connections to the access network, wherein said one or more egress boundary routers transmit intra-VPN traffic toward the destination host via the first logical connection and transmit extra-VPN traffic toward the destination host via the second logical connection (paragraph 0046; paragraph 0069; paragraph 0089); a plurality of ingress boundary routers coupled to the one or more egress boundary routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic (Fig. 5paragraph 0046;), such that denial of service attacks on said access link originating from sources outside the VPN can be prevented (paragraph 0084; paragraph 0090-0093).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Liu such that a denial of service attack is prevented. One of ordinary skill in the art would have been motivated to do this because it would prevent a bandwidth consumption attack (Tabata: paragraph 0084).

Referring to Claim 16:

Liu discloses a method of protecting an access link to a destination host belonging to a virtual private network (VPN) against denial of service attacks, said method comprising: in an access network including the access link, providing a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN traffic from sources outside the VPN (col 7, lines 25-45);

Liu does not explicitly disclose "communicating, from a plurality of ingress boundary routers to one or more egress boundary routers, intra-VPN and extra-VPN traffic destined for said destination host, wherein said intra-VPN traffic and said extra-VPN traffic are transmitted utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic; transmitting intra-VPN traffic from said one or more egress boundary routers toward the destination host via the first logical connection, and transmitting extra-VPN traffic from said one or more egress boundary routers toward the destination host via the second logical connection, such that denial of service attacks on said access link originating from sources outside the VPN can be prevented."

Tabata discloses communicating, from a plurality of ingress boundary routers to one or more egress boundary routers, intra-VPN and extra-VPN traffic destined for said destination host (Fig. 5; paragraph 0046), wherein said intra-VPN traffic and said extra-VPN traffic are transmitted utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic (paragraph 0064; paragraph 0069); transmitting intra-VPN traffic from said one or more egress boundary routers toward the destination host via the first logical connection, and transmitting extra-VPN traffic from said one or more egress boundary routers toward the destination host via the second logical connection (paragraphs 0071-0073), such that denial of service attacks on said access link originating from sources outside the VPN can be prevented (paragraph 0084).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Liu such that a denial of service attack is prevented. One of ordinary skill in the art would have been motivated to do this because it would prevent a bandwidth consumption attack (Tabata: paragraph 0084).

Referring to Claim 21:

Liu discloses a method for resisting denial of service attacks on an access link to a destination host included in a VPN, the method comprising the steps of: intra-VPN traffic flowing from sources included in the VPN (col 7, lines 25-45); extra-VPN traffic flowing from sources outside the VPN (col 7, lines 25-45);

Liu does not explicitly disclose "assigning a first priority level to traffic intra-VPN traffic flowing from sources included in the VPN; assigning a second priority level to traffic extra-VPN traffic flowing from sources outside the VPN; and granting, to traffic having the first priority level at the access link, precedence of access to the destination host over traffic having the second priority level."

Tabata discloses assigning a first priority level to traffic intra-VPN traffic flowing from sources included in the VPN; assigning a second priority level to traffic extra-VPN traffic flowing from sources outside the VPN; and granting, to traffic having the first priority level at the access link, precedence of access to the destination host over traffic having the second priority level (paragraph 0089).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Liu such that precedence information

is used to partition the traffic. One of ordinary skill in the art would have been motivated to do this because it would prevent a bandwidth consumption attack (Tabata: paragraphs 0084-0087).

Referring to Claims 2, 10 and 17:

Liu in view of Tabata disclose the limitations of Claims 1, 9 and 16 above. Tabata further discloses a Differentiated Services network coupling at least one of the plurality of ingress boundary routers and at least one of the one or more egress boundary routers (paragraph 0063).

Referring to Claims 3 and 11:

Liu in view of Tabata disclose the limitations of Claims 1 and 9 above. Liu further discloses a plurality of customer premises equipment (CPE) edge routers each coupled to a respective one of said plurality of ingress boundary routers (col 5, line 60-col 6, line 10).

Referring to Claim 4:

Liu in view of Tabata disclose the limitations of Claim 1 above. Liu further discloses further comprising the access network (Fig. 1).

Referring to Claims 5 and 12:

Liu in view of Tabata disclose the limitations of Claims 4 and 9 above. Liu further discloses a customer premises equipment (CPE) edge router to the access link (Fig. 1; col 6, lines 1-25).

Referring to Claims 6, 13 and 18:

Liu in view of Tabata disclose the limitations of Claims 5, 12 and 16 above. Tabata further discloses said CPE edge router having a physical port coupled to said access link, said physical port implementing a first logical port for intra-VPN traffic and a second logical port for extra-VPN traffic (paragraph 0069).

Referring to Claims 7, 14 and 19:

Liu in view of Tabata disclose the limitations of Claims 1, 9 and 16 above. Tabata further discloses at least one of said plurality of ingress boundary routers implements a plurality of tunnels that logically partition intra-VPN and extra-VPN traffic (paragraph 0108).

Referring to Claims 8, 15 and 20:

Liu in view of Tabata disclose the limitations of Claims 1, 9 and 16 above. Tabata further discloses said one or more egress boundary routers provide a plurality of different qualities of services to said intra-VPN traffic (paragraph 056-0058; paragraph 0101).

Conclusion

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:00am - 4:30pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TAG
12/13/04

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100